(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
1 juillet 2004 (01.07.2004)

PCT

(10) Numéro de publication internationale
WO 2004/055665 A1

(51) Classification internationale des brevets[7] : G06F 7/72

(21) Numéro de la demande internationale :
PCT/FR2003/003681

(22) Date de dépôt international :
11 décembre 2003 (11.12.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/15623 11 décembre 2002 (11.12.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue Du Pic De Bertagne, Parc D'activités De Gèmenos, F-13420 (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(pour US seulement)* : **JOYE, Marc** [FR/FR]; 19 rue Voltaire, F-83640 SAINT ZACHARIE (FR).

(74) Mandataire : **BRUYERE, Pierre**; C/O GEMPLUS, Service Brevets, LA VIGIE, BP 90, F-13705 LA CIOTAT CEDEX (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) **Title:** METHOD FOR SECURE INTEGER DIVISION OR MODULAR REDUCTION AGAINST HIDDEN CHANNEL ATTACKS

(54) **Titre :** PROCEDE DE DIVISION ENTIERE OU DE REDUCTION MODULAIRE SECURISE CONTRE LES ATTAQUES A CANAUX CACHES

(57) **Abstract:** The invention concerns a cryptographic method which consists in performing a integer division of the type q = a div b and/or a modular reduction of the type r = a mod b, with q being a quotient, a being a number of m bits, b being a number of n bits, n being not more than m and b_{n-1} non null, b_{n-1} being the most significant bit of the number b. The invention is characterized in that it consists in masking the number a by a random number ρ before performing the integer division and/or the modular reduction. The invention also concerns an electronic component for implementing said method. The invention is applicable for making secure smart cards against hidden channel attacks, and in particular differential attacks.

(57) **Abrégé :** L'invention concerne un procédé cryptographique au cours duquel on réalise une division entière de type q = a div b et / ou une réduction modulaire de type r = a mod b, avec q un quotient, a un nombre de m bits, b un nombre de n bits, n inférieur ou égal à m et b_{n-1} non nul, b_n-1 étant le bit de poids le plus fort du nombre b. Selon l'invention, on masque le nombre a par un nombre aléatoire p avant de réaliser la division entière et / ou la réduction modulaire. L'invention concerne également un composant électronique pour la mise en oeuvre du procédé ci-dessus. Application à la sécurisation des cartes à puce contre les attaques à canaux cachés, et notamment les attaques différientielles.

WO 2004/055665 A1